Office of Information Technology

NIH - Office of Director - Executive Office

Customer Service Newsletter

Fall Edition 2003

****

A Word from the OIT Director & CIO-OD

As October 1 approaches, OD and the other NIH ICs will reach a milestone per completing the FY-03 IT Consolidation at NIH. Except for having to live with a smaller mailbox, OD & NCMHD staffs have not experienced major impacts. I anticipate that information will be released during the Fall on the next phase of the HHS IT consolidation that NIH will have to implement.

The end of summer brought other IT issues to the surface. The article on Security Awareness below is important given the OD & NCMHD desktops that were infected with one of the recent worms. OIT is working to implement an improved system to ensure all desktops and laptops receive protection via an efficient mechanism. The hurricane and late summer thunderstorms once again caused a long power outage at 6011 Executive Blvd. The OD-ITMC approved moving critical OD web sites from 6011 to Building-31 before the arrival of Isabel. OIT will be implementing a process to ensure all OD & NCMHD web sites are at a location where electricity remains during storms.

"Computers are definitely smarter than people. When's the last time you heard of six computers getting together to form a committee?"

****

Customer Relationship Management Team (CRM)

Are Spammers using Chain Letters to get your email address?

Are you being cursed with chain letters and spam emails? Computer experts are warning their customers against chain letters--they suspect spammers are collecting email addresses used in these letters. This method is not as efficient as "spiders" that will automatically slither through the web searching for addresses but it does work. When you forward a chain letter to all of your friends and they send it to their friends, the spammers can collect all of these email usernames!

Protect Yourself!
The key to protecting yourself is to keep your email addresses as private as you can. When you receive chain letters, you should delete them from your system before opening them and ask your friends to stop sending you chain letters. This will keep your email address from showing up as the chain letter grows from person to person.

Remember! If your email address is randomly being sent from person to person, then it's out there for spammers to find!

Survey Statistics	Jun- 03	Jul - 03	Aug - 03
Surveys Sent	584	457	614
Surveys Received	154	125	161
Percentage Received	27%	30%	38%
Overall Score	3.81	3.87	3.85

****

Security Awareness

Protect your computer from Viruses!

With the recent W32.Blast.Worm, and the SoBig Worm exploit within NIH, we thought it would be a good idea to explain the various forms of malicious code, now commonly known as malware, and how they operate.

What is malware?
Malware – short for malicious software – refers to any malicious or unexpected program or code such as viruses, Trojans, and droppers. Not all malicious programs or codes are viruses. Viruses, however, occupy a majority of all known malware to date including worms.

What is a Trojan?
A Trojan is malware that performs unexpected or unauthorized, often malicious, actions. Unlike viruses, Trojans cannot replicate. Trojans cause damage, unexpected system behavior, and compromise the security of systems, but do not replicate.

What is a Virus?
A computer virus is a program – a piece of executable code – that has the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of file and are spread as files that are copied and sent from individual to individual.

In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. If the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

Several years ago, most viruses spread primarily via floppy disk, but the Internet has introduced new virus distribution mechanisms. With email now used as an essential business communication tool, viruses are spreading faster than ever. Viruses attached to email messages can infect an entire enterprise in a matter of minutes, costing companies millions of dollars annually in lost productivity and clean-up expenses.

Eradication
If enough users install up-to-date virus protection software, any virus can be wiped out. So far no viruses have disappeared completely, but some have long ceased to be a major threat.

What can you do to Protect against malware?
At the top of the list is using an antivirus product, and keeping it up-to-date with the latest pattern files. OIT has pushed virus update signature files to PCs connected to the OD LAN.

CIT posts the latest signature files at http://sdp.cit.nih.gov/downloads/antivirus.asp. The process is pretty straightforward. However, if you have any questions, you can always call the NIH Help Desk. Also, keeping your systems properly patched is extremely important. Malware code attacks known system vulnerabilities. A properly patched system renders the attack powerless. OIT is seeking a centralized way of keeping all desktops patched and current. If you connect remotely via a government issued laptop or desktop, you can bring it to work at least twice a year for OIT to perform a security checkup. Contact the NIH Help Desk to have an OIT Technician assist you.

The recent attack on NIH and communities around the world reveals two very important points.

1) How dependent we are on computers in our everyday lives.

2) How so very important it is to protect our systems through antivirus software and system patch updates.

Please continue to do your part in keeping our systems operational as well as malware and virus free.

****

Desktop Support Team

BlackBerry – Did You Know?

Did you every wonder what a BlackBerry Pin was? How about setting your password or maybe what to do if you ever lose your BlackBerry? Below are a few quick frequently asked questions about the BlackBerry. For more information, click on this link to our OIT Web site:

http://oit.od.nih.gov/pubs/crm/blackberryFAQ.pdf

1) Is it safe to use my handheld outside while it's raining or snowing?

While a few drops of moisture should not damage your handheld, you should avoid placing it in direct contact with liquids.

2) I've noticed the word PIN on the handheld, in the BlackBerry Desktop Software, and in the documentation. What is it?

PIN is short for Personal Identification Number. Each handheld has a unique PIN, like every phone line has a unique phone number. PINs are up to 8 digits long.

If you know the PIN of another BlackBerry handheld, you can send messages directly to that PIN rather than to the person's email address. Enter the PIN in the address entry for that person and select Use PIN when you send the message.

You can find your PIN by selecting the Options icon, then selecting Status. Your PIN appears in the Status screen. Your PIN is also displayed in the BlackBerry Desktop Redirector and in the BlackBerry Desktop Manager.

3) My BlackBerry handheld was lost or stolen. What can I do to ensure that someone else will not be able to send or receive messages with it?

If your BlackBerry handheld has been lost or stolen you can phone 1-877-255-2377 and give the PIN of your handheld to have it deactivated. HHS policy requires BlackBerry users to use a password on the BlackBerry. See Question 5 below.

4) The handheld screen is very faint. How do I adjust the screen contrast?

On your handheld, on the Home screen, click the Options icon.

- Click Screen/Keyboard.
- In the Screen Contrast field, press SPACE to scroll through the options or use the number keys to type the contrast.
- Release SPACE when the desired option is displayed or stop after you have typed in the desired contrast setting.
- Click the trackwheel and click Save.

5) How do I enable a password on my handheld?

One security feature of the BlackBerry handheld is the password option. If your handheld has a password enabled, the data on your handheld cannot be accessed until the correct password is typed. HHS policy requires you to password protect the BlackBerry.

To enable the password option, perform the following steps:

- On your handheld, on the Home screen, click the Options icon.
- Click Security.
- In the Password field, select Enable.
- You are prompted to type your new password twice, to verify the password.
- The Security Timeout field displays the amount of time after which the password is enabled when the handheld is inactive.
- Click the track wheel and click Save.

****

Network Operations Team

Requesting & Modifying Accounts for New or Transferring Employees

We would like to let everyone know about the *new* OD process for requesting and modifying computer accounts for new or transferring employees.

What are we talking about?

Accounts need to be created for new or transferring employees so that they can log in to the OD network, access email, and access files over the network. Also, when employees move, our directories need to be updated with the new information (e.g., address, phone, etc.).

Who can make these requests?

Each employee in the OD has an Administrative Officer (AO), who handles, among other things, account information. AOs can request new accounts, modifications of existing accounts, and account removal. The AOs can designate alternates to handle this task as well. These requests are made through a specially designed Outlook form, located in a Public Folder, which only AO's and their alternates can access. If you need your information updated, please contact your Administrative Officer.

I'm an AO, and I never heard of this!

If you are an AO and need access to our account request forms, please contact the NIH Helpdesk, and they will route your request to us. (A presentation on this process was made at an OD-AO meeting.)

Need more information? Feel free to contact the NIH Helpdesk, and they will get all of your questions to us.

****

Web & Development Team

How to search the World Wide Web - Keyword Search Operators

Operators are the rules or specific instructions used for composing a query in a keyword search. A well-defined query greatly improves the chances of finding the information you are looking for. While each search engine has its own operators, some operators are used in common by a number of search engines. Two of the most commonly used operators are listed below, more can be found in the Web Tips and Tricks section of our web site at:

http://oit.od.nih.gov/pubs/crm/HowToSearchWWW.pdf

1) Boolean

Uses "AND", "OR", "NEAR" and "NOT" to connect words and phrases [i.e. terms] in the query where:

- **AND** requires that both terms are present somewhere within the document being sought.
- **NEAR** requires that one term must be found within a certain number of words of the other term.
- **OR** requires that at least one of the terms is present.
- **NOT** excludes any document containing the term.

When using these operators, remember to capitalize them as shown above.

Query Example: search **AND** tutorial

2) Plus / Minus

- Uses [+] before a term to retrieve only the documents containing that term. It is similar to the Boolean AND.
- Uses [-] before a term to exclude that term from the search. It is similar to the Boolean NOT.

Do not leave a space between the operator and the term that follows.

Query Example: +search +tutorial –course

****

Tips N Tricks

Need to Upgrade your System/Equipment?

The OIT Desktop Team has created a checklist to assist you in requesting information about upgrading your system/equipment. Visit the OIT website at: http://www1.od.nih.gov/odeqchecklist/index.asp . Complete the checklist, starting with "Requestor's Name." Click on the "*submit"* button in the lower left corner and an email will be sent to the OIT Desktop Team. The Desktop Team will evaluate your requirements and provide you with three specifications, i.e. low, medium and high. In addition, this will ensure that the system/equipment you procure will be compatible with the existing OD network computer environment.

For more tips like this see the back of our "Guide to OD Computing" handout or go to the guide on our web site at: http://oit.od.nih.gov/pubs/oitguidebook.pdf

****

How Are We Doing?

Listed below are our performance measures for the Customer Satisfaction Survey that began April 24th, 2002. If our performance falls below a  , an explanation of the steps being taken to improve will be provided.

Network Support.....		Desktop support.....	
Web/Application support.....		Overall OD/OIT support.....	

 = available when I need it and/or exceeded service level agreement for call resolution.

 = not available when I need it and/or did not meet service level agreement.

Your feedback is very important to us. It helps identify areas needing improvement and acknowledges superior service.

Customer Support Points of Contact

Levels Of Escalation:

NIH Help Desk	(301) 594-3278	CRM Team Lead	Sue O'Boyle
CIO-OD & OIT Director	David Wiszneauckas	Desktop Team Lead	Marcelo Coelho
Chief Technology Officer	William Kibby	Web & Dev Team Lead	Daniel Williams
IT Policy/ITS Budget	Angela Murphy	Network Team Lead	Minh Chau
ISSO	Antoine Jones		